UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/005,733 90/005,776 09/694,416	05/18/2000	5848259	C72370US	7105

7590 06/21/2002

LEAH SHERRY
OPPENHEIMER, WOLFF, & DONNELLY, LLP
1400 PAGE MILL AVENUE
PALO ALTO, CA 94304

EXAMINER	
James Seal	
ART UNIT	PAPER NUMBER
2131	19

DATE MAILED: 06/21/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

09694416 . 062102

PTO-90C (Rev. 07-01)

Office Action Summary	Application No.	Applicant(s)	
	09/694,416 90/005,776; 90/005,733	COLLINS ET AL.	
	Examiner	Art Unit	
	James Seal	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 April 2001* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-61* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

15)☒ Notice of References Cited (PTO-892)
16)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
17)☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
18)☐ Interview Summary (PTO-413) Paper No(s). _____ .
19)☐ Notice of Informal Patent Application (PTO-152)
20)☐ Other: .

DETAILED ACTION

1. Application 09694416 is a reissue of patent US 5848159 A and has been merged with reexamination proceedings 9005733 and 9005776, MPEP 2285.

2. The original patent, or an affidavit or declaration as to loss or inaccessibility of the original patent, must be received before this reissue application can be allowed. See 37 CFR 1.178. This is a reminder, the offer to surrender is on file.

3. In accordance with 37 CFR 1.175(b)(1), a supplemental reissue oath/declaration under 37 CFR 1.175(b)(1) must be received before this reissue application can be allowed. Any substantive amendments require a supplemental declaration. This declaration can be submitted at the end of prosecution. This is a reminder that a single oath should be submitted at the end of prosecution.

4. This application is objected to under 37 CFR 1.172(a) as lacking the written consent of all assignees owning an undivided interest in the patent. The consent of the assignee must be in compliance with 37 CFR 1.172. See MPEP § 1410.01.

A proper assent of the assignee in compliance with 37 CFR 1.172 and 3.73 is required in reply to this Office action.

5. The copy of the assignment submitted is from TANDEM COMPUTERS INCORPATED. However, the oath lists Compaq Computer Corporation as the Assignee. Submission of an assignment to Compaq is required.

Drawings

6. New formal drawings are required in this application. The office no longer transfer drawing from the patent to the reissue.

Amendment

7. Amendments filed 19 October 2000 have been entered

8. Supplemental IDS dated 11 April 2001 and 26 June 2001 have been considered. Signed copy is enclosed.

9. Claims 1-61 are pending.

Specification

10. The amendment filed 11 April 2001 is objected to under 35 U.S.C. 132 because it introduces new matter into the disclosure. 35 U.S.C. 132 states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: Page 6 paragraph beginning at Col 5, line 52 includes a digital signature. Digital signatures were not disclosed in original specification as was originally filed and are not necessarily a consequence of a public key cryptosystem. In fact a number of public key system, such as Diffie-Helmann, Merkle's Puzzles, RSA type 0 elliptic curve, and Knapsack can not incorporate digital signatures into their make up.

Applicant is required to cancel the new matter in the reply to this Office Action.

11. The disclosure is objected to because of the following informalities:

12. The correction to equation (4) column 2 line 22 submitted in the amendment of 19 October 2000 is incorrect. The equation in the original patent only requires "=" to be changed to "≡".

13. Page 11, second paragraph of the amendment filed 19 October 2000, seeks to replace "20 initiates write operations to address within the memory space ..." with "In similar fashion, information is conveyed to ..."; however that paragraph begins at line 62. Applicant is requested to confirm this.

Claim Objections

14. The amendment submitted 19 October is objected to because of the following informalities:

15. In line 19 (page 14) of amended claim 3 submitted 19 October 2000, seeks to replace $0 \leq M_A" \leq n_B - 1$ with $0 \leq M_A" \leq n_2 - 1$; however, this is incorrect and should be replaced by $0 \leq M_1" \leq n_2 - 1$ to be consistent with other changes in the claim.

16. In the last line of amended claim 3 (page 14) submitted 19 October 2000, seeks to replace $C_A \equiv M_A"^{e_B} \bmod n_B$ with $C \equiv M_1"^{e_1} \bmod n_2$ is incorrect and should be replaced by $C_1 \equiv M_1"^{e_2} \bmod n_2$ as the first terminal should use the public key of the second terminal.

17. Appropriate correction is required.

Claim Rejections - 35 USC § 101

18. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

19. Claims 7-8 and 13 are rejected under 35 U. S. C. 101 because the claimed invention lacks patentable utility is not supported by either a creditable and substantial asserted utility or a well established utility.

20. The invention as understood by the examiner is directed to a system/method for increasing the computation speed of standard RSA

$$C \equiv M^e \bmod n \qquad M \equiv C^d \bmod n$$

$$ed \equiv 1 \bmod L \quad n = pq \quad L = \text{lcm}\{p-1, q-1\} \quad 0 \leq M \leq n-1$$

where M is the plaintext message, C is the ciphertext, e is the public key, and d is the decryption key and lcm{...} is the least common multiple of the arguments (Column 5, line 9, Column 8, lines 30-32, Column 13, line 1). It should be noted that for two distinct primes, this is equivalent (though not necessarily equal, in the sense of Euler's theorem) to $\phi(n) = (p-1)(q-1)$, that is $ed \equiv 1 \bmod \phi(n)$ which is found in so many references on two prime RSA. We shall continue to use L as this is the form Rivest uses in their patent.

By choosing a modulus consisting of the product of distinct multiple primes $p_1\ p_2\ p_3 \ldots p_k$ where $k \geq 3$ and then using the Chinese Remainder Theorem (henceforth, CRT) to break up the results into k first order congruencies which may be calculated simultaneously and recombined by the Chinese Remainder theorem to produce the results. The increased speed is the results of two different aspects: the multi- prime moduli and the fact that the CRT allows calculations to be placed into parallel both of which are interrelated (see Knuth, volume 2). The first aspect allows the size of the

numbers entering into the calculations to be decreased by a factor k, which in the case of k = 2 means 1/2, and an effective gain of 2 in the speed. The CRT allows a single exponentiation to be broken down into k congruencies that are independent of one another and hence be calculated in parallel. Combining these two aspects of the CRT make the run time about ¼ of the standard RSA.

Now looking at Claim 7, the applicant claims an encryption algorithm of the form

$$C \equiv (a_e M^e + a_{e-1} M^{e-1} + \ldots + a_0) \bmod n$$

Where $a_0, a_1, a_2, \ldots a_e \in Z_n$ and n is a product of distinct primes $p_1, p_2, p_3, \ldots p_k$.

In Claim 8, applicant recites the steps of decryption. The claimed method of decryption fails to provide an enabling disclosure for decryption of the encryption algorithm as specified in claim 7. Decryption by definition is the invertible complement to the encryption operation. The examiner asserts that mere recitation of a method of invertible operations in and of itself, does not give rise a recitation of utility and/or enables the invention as recited in claim 7.

21. The examiner asserts that an invention which is useful for encryption only fails to provide utility because a message which cannot be decrypted is of no use to a sender or a receiver.

Claim Rejections - 35 USC § 112

22. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

23. Claims 8 and 13 rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

24. Alternatively, if the encryption algorithm as recited in claim 7

$$C \equiv \sum a_i M^i \bmod n$$

is suppose to correspond to the decryption recited in claim 8, that is the performance of a first ordered *succession* of invertible operations on M for which the decryption corresponds to a second ordered succession of invertible operations on C. There is no disclosure as to how this set of invertible succession of operations comes about from the encryption algorithm given above.

25. Further, in general solving for M given n and C is not possible. This is equivalent to solving the problem

$$f(M) \equiv C - \sum a_i M^i C \equiv 0 \bmod n$$

This equation is over the field of integers mod n i.e. Z_n and is not as simple as solving this same equation for the field of real numbers $\mathbb{R}$. This equation can be inverted only if there exist an M for which the simultaneous set of congruencies

$$f(M) \equiv 0 \bmod p_1$$

$$f(M) \equiv 0 \bmod p_2$$

$$f(M) \equiv 0 \bmod p_3$$

...

$$f(M) \equiv 0 \bmod p_k$$

has a solution in M. Further even if this condition is satisfied, this does not guarantee that a succession of invertible operations exist. Thus, it is doubtful whether one of ordinary skill in the art could practice this invention as recited.

26. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

27. Claims 24-25, 26-28, and 29-39 are rejected under 35 U.S.C. 112(2)

28. Claims 26-27, 29, 31, and 33 are rejected under 35 U.S.C. 112(2) recites because of the recitation of "faster than heretofore possible" which is a relative term without a standard with which to compare.

29. Claims 24, 25, 28, 30 and 32 are rejected under under 35 U.S.C. 112(2) recites "fewer computational cycles" which is a relative term without a standard with which to compare.

30. Claims 34-39 are rejected under 35 U.S.C. 112(2) recites "compatible with two-prime RSA public key cryptography". It is not clear in what sense or what configuration is being defined by the word *compatible*.

Claim Rejections - 35 USC § 102

31. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

32. Claims 1-61 rejected under 35 U.S.C. 102(b) as being anticipated by Rivest et. al. (US 4,405,829 A) henceforth Rivest.

33. As per claim 1, the limitation of a method for processing messages in a communication communitication system (see Figure 6, Abstract line 1 of Rivest), such that the encryption algorithm is given by $C \equiv M^e \bmod n$ (Column 4, line 59, Rivest) where $0 \leq M \leq n-1$ (Column 4, line 26) is the plaintext message (Column 4, lines24-25) and C is the corresponding ciphertext (Column 4, lines 20-21). The examiner first notes that Rivest in Column 13, lines 29-34 states "a modulus n of three or more primes (not necessarily distinct)", i.e., $n = p_1p_2p_3...p_k$. However, in order to apply the Chinese Remainder theorem (CRT) the primes must be relatively primed in pairs implying their distinctness. Rivest "Decoding may be performed modulo each of the prime factors of n", that is, with respect to mod p_1; mod p_2; mod p_3; ... mod p_k. Claim 1 is rejected.

34. As per claim 2, the limitation that the decryption of the ciphertext C, should be accomplished by $M \equiv C^d \bmod n$ is disclosed Column 13, lines 44-46 and d is chosen as the multiplicative inverse of e such that $ed \equiv 1 \bmod L$ (as noted above, L is the least common multiple, and in the multi prime case is given by $L = \text{lcm} \{ p_1 - 1, p_2 - 1, ... p_k - 1 \}$). Claim 2 is rejected.

35. As per claim 3, the limitation of j communicating terminals on a communication system, with encrypting key $E_i = (e_i, n_i)$ and decryption keys $D_i = (d_i, n_i)$ i = 1, 2, ... j, (Column 8, lines 22-27) wherein for each terminal i, e_i, d_i, and n_i are defined as in claims 1 and 2 (see above) wherein the message M_i corresponding to a number

representative of a message-to-be-transmitted from the ith terminal and in particular terminal 1 transmits a message M1 to terminal 2 by breaking the message M into blocks M" where $0 \leq M_1" \leq n_2 - 1$ (Column 4, lines 31-35; Column 8, line 39) message to ciphertext using $C \equiv M_1"^{e2} \bmod n_2$ (Column 8, line 56). Claim 3 is rejected.

36. As per claim 4, the limitation that the decryption of the ciphertext C between two terminals (as defined in claim 3) is decrypted according to $M' \equiv C^d \bmod n$ (where d and n are defined as above) and where M' corresponds to the decoded ciphertext block is disclosed (Column 8, line 43). Claim 4 is rejected.

37. As per claim 5, the limitation of a communication system incorporating the encryption of messages as claim 3 and the receipt and decryption of messages as claim 4 form a *first* (or transmitting) terminal to a second terminal and are therefore rejected on grounds analogous to those used to reject claims 3 and 4.

38. As per claim 6, the limitation of a communication system incorporating the encryption of messages and the decryption of messages from a second (transmitter) terminal to a first terminal (receiver) and a blocking means (Column 4, line 33) and are therefore rejected on grounds that the limitations of claim 6 combine the limitations of claims 3 (an encoder for encrypting messages to be transmitted) and 4 form (decoding messages encrypted in the manner of three) and are rejected in view of the same art of record.

39. As per claim 7, the limitation of processing encrypting messages M where $0 \leq M \leq n - 1$ into ciphertext C, and such that the ciphertext is generated from the plaintext as follows:

$$C \equiv a_e M^e + a_{e-1} M^{e-1} + \ldots + a_0 \mod n$$

where e, a_e, a_{e-1}, ... a_0 are numbers is disclosed by Rivest Column 13, lines 36-39. Claim 7 is rejected.

40. As per claim 8 to the extent understood by the examiner, Rivest discloses the use of root finding techniques (Column13, line 39-40), to find a representation of C in terms of an ordered succession of invertible operation (modulo n) on M (Column 13, lines 56-58). Claim 8 is rejected.

41. As per claims 9 and 10, the limitation of sending signed messages between terminals is disclosed by Rivest Column 5, lines 18-50 and Column 8 lines 56-67. Claims 9 and 10 are rejected.

42. As per claim 11, the limitation that the communication system is comprised of stations capable of generating ciphertext is disclosed by Rivest Column 8, lines 33-39 and Column 10, line 28-34. Claim 11 is rejected.

43. As per claim 12, the limitation that such stations transmit ciphertext is disclosed by Rivest Column 8, lines 33-39, Column 10, lines 11-24, lines 28-34, and Figure 4. Claim 11 is rejected.

44. As per claim 13, the limitations that a communication system has stations in the manner of claim 11 for encryption/decryption messages which is carried out according to claims 7 and 8 is therefore rejected on the grounds analogous to those used to reject claims 7, 8 and 11.

45. As per claims 14 and 15, a method of processing messages by *selecting* a public e which is used with the relationship $C \equiv M^e \mod n$ (claim 14) and (claim 15)

establishing a private key portion $d \equiv e^{-1} \bmod L$ respectively is disclosed by Rivest Column 6, lines 21-37. Claims 14 and 15 are rejected.

46. As per claim 16, a method of processing messages selecting a public key e and establishing a private key $de \equiv 1 \bmod L$ where n is a product of 3 or more *distinct* primes and decoding ciphertext using the relationship $M \equiv C^d \bmod n$ is disclosed by Rivest Column 6, lines 21-37 and Column 13 lines 29-31, lines 41-43. Claim 16 is rejected.

47. As per claim 17, the limitation $M \equiv C^d \bmod n$ is disclosed by Rivest Column 13 line 46. Claim 17 is rejected.

48. As per claim 18, selecting a public key e and corresponding private key $d \equiv e^{-1} \bmod \phi(n)$ and encrypting M with the private key produces a signed message M_s is disclosed by Rivest Column 8 lines 56-67. claim 18 rejected.

49. As per claim 19, the limitation that the signed message can be verified by the public key is disclosed by Rivest Column 9, line 3. Claim 19 rejected.

50. As per claims 20-23, the limitations of a multiprime RSA cryptosystem n = pqrs... whereby the speed of the cryptographic process is increased is disclosed by Rivest Column 13, line 33. Rivest discloses the use of the CRT, which because of its mathematical form allows the breaking up of the decryption process into a series of subtasks ($M_p \equiv C^d \bmod p$; $M_q \equiv C^d \bmod q$; $M_r \equiv C^d \bmod r$; and $M_s \equiv C^d \bmod s$ ...). This puts the calculation in terms of subtask which are then automatically in a form to utilize

parallel processing in the calculation and because the primes used in each subtask are small, increased speed is a consequence. Claims 20-23 are rejected.

51. As per claims 24, 25, 28, 30, and 32, in as far as the examiner understands the limitation, "fewer computational cycles" for a multiprime RSA cryptosystem, is disclosed by Rivest as a results of the CRT as discussed above. With smaller primes, the necessary computational cycles would also be less, for example using the Euclidean algorithm or the CRT. Claims 24, 25, 28, 30, and 32 are rejected.

52. As per claims 26, 27, 29, 31, and 33, in as far as the examiner understands the limitation, "faster than heretofore possible" for a multiprime RSA Cryptosystem is disclosed by Rivest as a results of the CRT as discussed above. If the number of computational cycles is fewer that would imply that the calculation are completely faster. Claims 26, 27, 29, 31, and 33 are rejected.

53. As per claims 34-39, in as far as the examiner understands the limitation, a "method compatible with RSA" with the multiprime RSA is disclosed by Rivest. Rivest would allow a standard two prime RSA cryptosystem to communicate with a multiprime RSA cryptosystem as only the public keys (e, n) are used for encryption by the other party machine and no use of the factorization is used in the process. Claims 34-39 rejected.

54. As per claims 40-41, the limitation of a cryptographic method for local storage of data by a private key is disclosed by Rivest Column 6 lines 50-57 and grounds in claims 14 and 15. Claims 40-41 rejected.

55. As per claim 42, the limitation of a communication system with a plurality of stations over a communication link (channel) is disclosed by Rivest Abstract.

56. As per claim 43, the limitation of a system for processing message by encrypting a first message $C \equiv M^e \bmod n$ and also being able to decrypt a second encrypted message C' into M' is disclosed by Rivest (see Figure 4). Claim 43 is rejected.

57. As per claims 44 and 45, the limitation of breaking the encryption/decryption into subtasks is a consequence of the application of the CRT which Rivest discloses in Column 13 line 33. Claims 44 and 45 rejected.

58. As per claim 46-49, the limitations of data bus (Figure 3), processor(Figure 3), memory (Figure 1&3), exponentiator (Figure 3, element 22) parallel processing (Column 13, line 33) is disclosed by Rivest Column 9, lines 6-58; Figure 3. DES implementation for session keys is disclosed by Rivest (Column 3, lines 23-30 and Column 1, lines 42-45, Column 14, lines 26-28). Claims 46-49 rejected.

59. As per claims 50-55, limitations involving subtasks is a consequence of the CRT which breaks up the decryption process ($M_p \equiv C^d \bmod p$; $M_q \equiv C^d \bmod q$; $M_r \equiv C^d \bmod r$; and $M_s \equiv C^d \bmod s$ ...) into subtask (Column 13, lines 31-34) disclosed by Rivest. Claims 50-55 are rejected.

60. As per claims 56-61, it would be inherent that Rivest would provide a means of key development or key generation in order to prevent degrading of security of the encryption system from overuse of keys. Claims 56-61 are rejected.

61. Claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, 50-57, 60-61 rejected under 35 U.S.C. 102(b) as being anticipated by Vanstone and Zuccherato (*Using four-prime RSA in which some bits are Specified*, Electronic Letters, 30(25), 16 August 1994).

62. Vanstone et. al. discloses an device for reducing key size for transmission to a group of users in a communication system using 4 primes RSA for increased speed and security (Vanstone et. al., column 1, page 2118,). Vanstone system is in response to the recently advances in factoring which make integers n, in the range $2^9 = 512$ bits insecure and suggests going to $2^{10} = 1024$ bits with 4 randomly selected primes, each prime contains about 250 bits in both cases (Column 1, first four sentences). There is nothing in the Vanstone method which precludes extending to more bits or more primes in order to address future security needs. Vanstone selects random primes even though he makes bit assignments in an expanded product. Vanstone further discloses use of the CRT for decryption ($M = C^d \bmod n$, $0 \leq M \leq n - 1$), which because of its mathematical form of breaking the decryption process into a series of subtasks ($M_p \equiv C^d \bmod p$; $M_q \equiv C^d \bmod q$; $M_r \equiv C^d \bmod r$; and $M_s \equiv C^d \bmod s$) allows implementation of parallel processing in the calculation. Furthermore the form of the CRT indicates that the primes are distinct. Claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, 50-57, 60-61 rejected.

63. Claims 1-6, 9-12, 14-31, 34-36, 38-44, 50-61 rejected under 35 U.S.C. 102(e) as being anticipated by Captian Nemo (RSA Moduli Should Have 3 Prime Factors). The Captain Nemo article was submitted in the original Collin's application, and although no

publication date mentioned in the parent case, the footnote at the bottom of the first page of the article, list a date of August 1996.

64. Nemo discloses an apparatus/method for use in networks and smartcard of using 3 primes (three primes) RSA for increased speed (section 4.1) and security (section 5) applicable to networks (section 4.2) using digital signature for validation (section 4.2, last paragraph and section 6) in a standard digital architecture (section 4.1). The speed increase due to the CRT and smaller moduli see Section 3.1 and 4, in particular parallel processing using subtasks (see especially 3.1). Claims 1-6, 9-12, 14-31, 34-36, 38-44, 50-61 rejected.

65. Claims 1-6, 9-12, 14-31, 34-36, 38-44, 50-61 rejected under 35 U.S.C. 102(e) as being anticipated by Slavin (US 5,974151 A) 21 September 1999.

66. Salvin discloses a method of encrypted communication (Abstract) using four prime RSA $n = p_1xq_2,xp_1xq_2$, in which the four primes are selected at *random* and all of which *all are different values* (Column 7, lines 35-67in particular lines 37-38)and corresponding public and private keys e and d (see figure 3, Column 4, lines 31-38 applied to a network with a plurality of users (Figure 1). Salvin further discloses the use of the CRT to speed up the 4 prime decryption (Column 9, lines 44-47) whose speed is inherent from the breaking up the modular exponentiation into smaller primes and parallel subtask.

67. Claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, 50-61 rejected under 35 U.S.C. 102(b) as being anticipated by Itakura and Nakamura, A Public-Key

Cryptosystem Suitable for Digital Multisignatures, NEC Res. & Develop. No 71, October 1983.

68. Itakura et. al. discloses an apparatus/method for cryptographic communications using 3 randomly selected distinct primes RSA for which the encryption is carried out C ≡ M^e mod n and n = pqr and ed ≡ 1 mod (p-1)(q-1)(r-1) and where decryption is carried out by M ≡ C^d mod n where 0≤ M ≤ n-1 and capable of performing one or more digital signatures per document S ≡ M^d mod n (See page 4 section 3) for increased speed and security of digital multisignature applicable to public-key cryptosystem in conjunction with a communication system for a plurality of users (network, see Figure 1, see Abstract Electronic mail). Itakura et. al. use a random number key generator to develop keys (Figure 1, section 3.1) Claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, 50-61 rejected

Double Patenting

69. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

The subject matter claimed in the instant application is fully disclosed in the referenced copending application and would be covered by any patent granted on that copending application since the referenced copending application and the instant application are claiming common subject matter, as follows: multiprime RSA cryptosystem using the CRT and parallel processing to increase speed.

Furthermore, there is no apparent reason why applicant would be prevented from presenting claims corresponding to those of the instant application in the other copending application. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

70. Claims 9, 11-12, 35, and 50-55 are provisionally rejected under the judicially created doctrine of double patenting over claims 14-62 of copending Application No. 09328726. This is a provisional double patenting rejection since the conflicting claims have not yet been patented.

References Cited and Comments

71. The examiner would like to list a summary of prior art of record that is relevant to this case.

1. Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, *Cryptographic Communications System and Method*, (US 4,405,829 A) 20 September 1983.

2. Itakura and Nakamura, A Public-key Cryptosystem Suitable for Digital Multisignatures, NEC Res. & Develop. No 71, October 1983

2. S. A. Vanstone and R. J. Zuccherato, *Using Four-prime RSA in Which Some of the Bits are Specified, Electronics Letters*, 8th December 1994, Volumn 30 (35), pgs 2118-2119

3. Captian Nemo, RSA Moduli Should Have 3 Prime factors, August 1996.

4. Keith R. Slavin, Public key Cryptographic system Having Nested Security Levels (US5924151 A).

72. We shall further note that the use of the CRT to speed up calculations by placing operations in parallel, predates public key systems. Knuth in his famous book, Art of Computing, V2 1969, discussed the use of the CRT for increasing the calculation speed by placing operations in parallel (pages 248-250), as an alternative to doing arithmetic on large integer to split the process up into parallel task u mod m_1; u mod m_2; ...

u mod m_r instead of dealing with u and n = $m_1m_2m_3...m_n$ and then reconstructing u in terms of n via the Chinese Remainder theorem.

73. The encryption system of claims 7-8, and 13

$$. C \equiv (a_e M^e + a_{e-1} M^{e-1} + \ldots + a_0) \bmod n$$

where $a_0, a_1, a_2, \ldots a_e \in Z_n$ and n is a product of distinct primes $p_1, p_2, p_3, \ldots p_k$ is further not a public key cryptosystem as it does not possess a decryption key d which is relatable to a public key through some process related to a trapdoor function, even through the title "Public Key Cryptographic Apparatus and Method" would seem to imply the opposite. .

Conclusion

74. Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes can be reached on 703 305 9711. The fax phone numbers for

the organization where this application or proceeding is assigned are 703 746 7239 for regular communications and 703 746 7240 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703 308 3900.

JWS

Jws
June 20, 2002

Gail Hayes

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100